Errata/Typos for “Introduction to Modern Cryptography, third edition”

(Last updated September 13, 2021)

Note: negative line numbers correspond to counting from the bottom of the page.

• page 362, Exercise 9.24: For this problem, assume that the twisted Edwards representation uses quadratic residue \( a \) and quadratic non-residue \( d \).

• page 577, line -7 should have “\( \geq \)” instead of “\( \leq \)” In any case, the only result we rely on is that when the \( \{ E_i \}_{i=1}^n \) are disjoint events with \( \Pr[\bigvee_{i=1}^n E_i] = 1 \), then for any event \( F \) we have

\[
\Pr[F] = \sum_{i=1}^n \Pr[F \wedge E_i] = \sum_{i=1}^n \Pr[F \mid E_i] \cdot \Pr[E_i].
\]

Thanks to Claude Crépeau for informing us about some of the above typos.